ISSN:0975-9646

Framework for Providing Security and Energy saving Using Elliptic Curve Cryptography in Wireless Sensor Networks

Venkateswarlu Sunkari [1]
Assistant Professor,
ITSC Department,
Addis Ababa Institute of Technology,
Addis Ababa, Ethiopia.

S. Kranthi Kumar [2]
Associate Professor,
Dept. of CSE, JSPM NTC College of Engineering , Nahre,Pune, Maharastra, India.

Ato Daniel Abebe[3]
HOD, ITSC Department,
Addis Ababa Institute of Technology,
Addis Ababa,
Ethiopia.

Abstract: In this recent years wireless sensors attracted the wireless sensor networks due to the significant advances in minimization. Wireless sensor networks consist of autonomous sensor nodes attached to one or more base stations. Wireless networks of low-power sensing devices are poised to become a ubiquitous part of the computing landscape. As Wireless sensor networks continues to grow, they become vulnerable to attacks and hence the need for effective security mechanisms. Due to these well accepted limitations, WSN is not able to deal with traditional cryptographic algorithms and symmetric based cryptographic schemes don't scale well when the number of sensor nodes increases. Sensor nodes should be resilient to attacks. Since WSN suffer from many constraints including low battery life, lower processing power, small memory and wireless communication channel. In this paper we propose an energy efficient secure framework that proves the integrity, authentication, and also provides secure communication among the sensor nodes by using the public key algorithm.

Index Terms: Wireless sensor networks, cryptography, low processing power, Encryption, Decryption, Public Key Cryptography.

I. INTRODUCTION

Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements. A Wireless Sensor Network (WSN) is composed of autonomous devices called sensor nodes that generally have low computational power, limited data transmission and power constraints. The field of sensor network is well known due to its popularity in research community. Wireless sensor networks are rapidly self configurable, deployable, and low cost and operate in absence of a pre-deployed infrastructure.

In the wireless sensor network various applications are used such as patient monitoring, smart homes, disaster relief, emergency rescue and industrial applications like environmental control, structural health and military applications like tracking and the target identification. The conversation between sensors nodes can be eavesdropped by the adversary .The adversary can be aware of the conversation between the sensors and can forge the data. Security is the main preconcern to socialize this network for common usage. The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior.

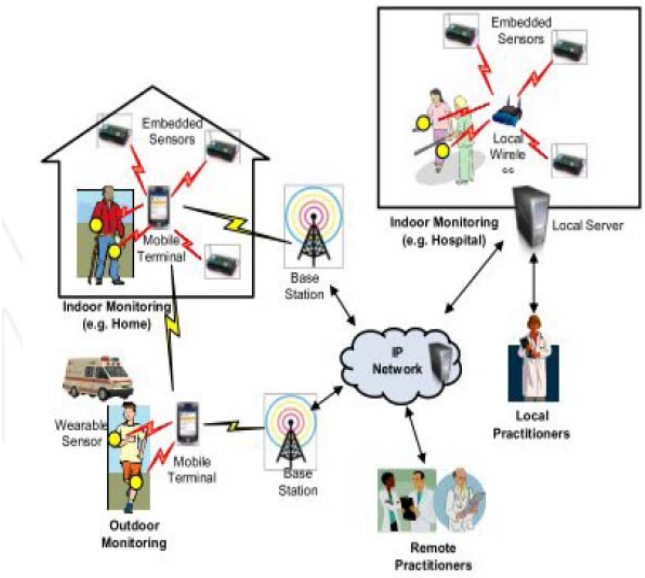

Fig.1: Wireless sensor networks

In sensor network security, an important challenge is the design of protocols to bootstrap the establishment of a secure communications infrastructure from a collection of sensor nodes which may have been pre-initialized with some secret information but have had no prior direct contact with each other. A bootstrapping protocol must not only enable a newly deployed sensor network to initiate a secure infrastructure. The difficulty of the bootstrapping problem stems from the numerous limitations of sensor networks like low battery life, lower processing power, wireless communication channels and small memory.

Most proposals rely on asymmetric digital signatures for the authentication, which are impractical for multiple reasons. The next issue is the security in sensor network. The security issues present for sensor networks have not been addressed at all in the protocol, where assurance does not provide for replay attack, confidentiality, and authentication. The critical problem is making effective use of that secure symmetric encryption capability. It is always the case with proper key management; symmetric encryption is a fundamental concern.

The security in sensor network will be employed by public key cryptography because it is easy to distribute keys in public key cryptography than symmetric key cryptography because of the random deployment of the sensor nodes in

the network. But a care should be taken for implementing public key cryptography in Sensor Network because of the constrained of sensor network devices. We are presenting a Public key algorithm using Elliptic Curve Cryptography algorithm for preventing replay attack in sensor network as well as for data confidentiality and authentication between sensor nodes.

II. BACKGROUND WORK

SECURITY:

The security is also independent upon the nature of applications and algorithm might be specified to the applications. The security requirements in WSN include:

Confidentiality: It is simply hiding the information from the unauthorized persons. Confidentiality ensures the concealment of the message from an attacker so that any message communicated via the sensor network remains confidential. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess. We set up secure channels between nodes and base stations and later bootstrap other secure channels as necessary

Authentication: Authentication ensures the reliability of the message by identifying its origin. Within the building sensor network, authentication is necessary for many administrative tasks. By authenticating other nodes, base stations and cluster heads before granting a limited resource, or revealing information. The issue of authentication should address the following requirements:

- Communicating node is the one that it claims to be
- The receiver should verify that the received packets have undeniably come from the actual sensor node

Integrity: Integrity ensures the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed while on the network. The issue of integrity should address the following requirements:

- Only the nodes in the network should have access to the keys and only an assigned base station should have the privilege to change the keys.
- It protects against an active, intelligent attacker who might attempt to disguise his attack as noise.

Availability: Availability ensures that services and information can be accessed at the time they are required. In the wireless sensor networks there are many risks that could result in loss of availability such as sensor node capturing and denial of service attacks**.**

Types of Security Attacks: There are two types of attacks namely: Active attacks and passive attacks.

Active Attack: This kind of attacks in which attackers in not only being able to listen the transmission but also being able to actively modify or generate false data. Types of active attacks are:

a. Masquerade
b. Replay
c. Denial of Service
d. Modification of Message

Passive Attack: A passive attack is an attack where an unauthorized user monitors or listens in on the communication between two parties.

Limitations of wireless sensor network:

There are many limitations in the wireless sensor network like limited bandwidth, limited resources etc. Some of the limitations are listed below:

- Vulnerability of nodes to physical capture
- Partial impracticality of public key Cryptosystems
- Lack of a-prior knowledge of post-deployment configuration
- Limited bandwidth and transmission power
- Limited memory resources
- Over reliance on base stations exposes
- vulnerabilities

III. EVALUATION METRICS

Several criteria that represent desirable characteristics for a bootstrapping scheme for sensor network. To secure our sensor network, we have broadly two schemes like symmetric and asymmetric cryptography.

Symmetric Cryptography: Symmetric encryption (also called as secret-key cryptography) uses a single secret key for both encryption and decryption as shown in Figure 2.

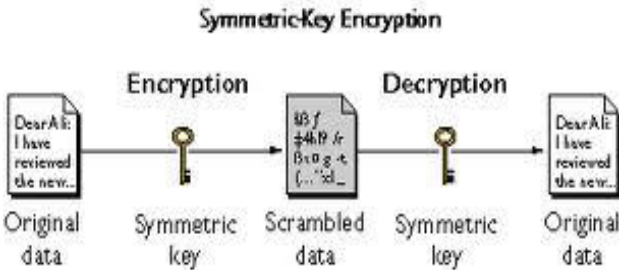

Fig.2: Symmetric key cryptography

This key has to be kept secret in the network, which can be quite hard in the exposed environment where WSNs are used to achieve the security requirements. Symmetric key algorithms are much faster computationally than asymmetric algorithms as the encryption process is less complicated. We first focus on Symmetric Cryptography due to the assumption that symmetric cryptography has a higher effectiveness and require less energy consumption. *SPINS* - Perrig et al., 2001 proposed a security building block that is optimized for resource-constrained environments and wireless communication. SPINS has two secure building blocks: *SNEP* and *μTESLA*.

SNEP (Secure Network Encryption Protocol): SNEP provides security primitives: two-party data authentication, data freshness and data confidentiality with less communication cost. SNEP provides a number of unique advantages.

- It has low communication overhead since it only adds bytes per message.
- We avoid transmitting the counter value by keeping state at both end points like many cryptographic protocols it uses a counter.
- SNEP achieves even semantic security, a strong security property which prevents eavesdroppers from

inferring the message content from the encrypted message.

- The same simple and efficient protocol also gives us two-party data authentication, data freshness and data confidentiality with less communication cost.

The important security property is *semantic security* that ensures that an eavesdropper has no information about the plaintext.

µTESLA (The Micro version of Timed, Efficient, streaming, Loss-Tolerant, Authentication Protocol): µTESLA is a new protocol which provides authenticated broadcast for severely resource constrained environments. Scheme is resilient to node capture and possible to revoke key, but it is not scalable and the base station becomes the target of attacks. It does not provide a solution for denial of service (DoS) attacks when the malicious node keeps sending the request to negotiate a session key because one adversary can easily trigger a REPLAY attack and exhaust the energy in the sensor nodes. SNEP offers the following nice properties:

Semantic security: Since the counter value is incremented after each message, the same message is encrypted differently each time.

Data authentication: A receiver can be assured that the message originated from the claimed sender, if the MAC verifies correctly.

Replay protection & Data Freshness: To prevent the replaying the old message MAC uses the counter value.

*Low communication overhead***:** The counter state is kept at each end point and does not need to be sent in each message.

µTESLA: Authenticated Broadcast: Current proposals for authenticated broadcast are impractical for sensor networks. Most proposals rely on asymmetric digital signatures for the authentication that are impractical for multiple reasons. The recently proposed TESLA protocol provides efficient authenticated broadcast. TESLA is not designed for such limited computing environments as we encounter in sensor networks for three reasons.

- TESLA authenticates the initial packet with a digital signature. Digital signatures are too expensive to compute on our sensor nodes, since even fitting the code into the memory is a major challenge.
- TESLA has an overhead of approximately 24 bytes per packet. It is simply impractical to disclose the TESLA key for the previous intervals with every packet: with 64 bit keys and MACs.
- The one-way key chain does not fit into the memory of our sensor node. Pure TESLA is not practical for a node to broadcast authenticated data.

<u>Asymmetric Cryptography:</u> Cryptographic frameworks are based on two shared keys, private key for encryption and public key for decryption. The asymmetric cryptographic frameworks are further classified as ECC based, RSA based and Pairing based cryptographic frameworks. The private key is never exposed.

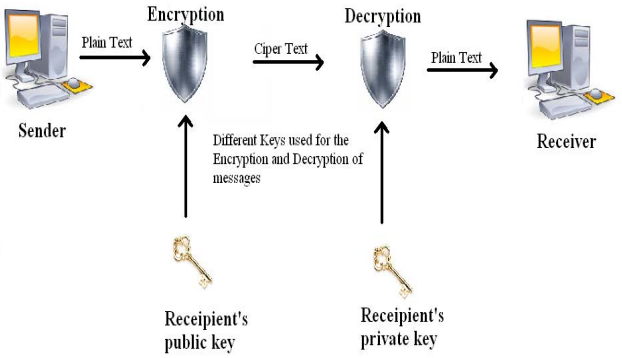

Fig.3. Asymmetric key Cryptography

The message that is encrypted by using the public key can only be decrypted by applying the same algorithm and using the matching private key. A message that is encrypted by using the private key can only be decrypted by using the matching public key. Public key Cryptography was omitted from the use in WSN because of its great consumption of energy and bandwidth which was very crucial in sensor network. In Public key Cryptography mostly two algorithms RSA and ECC use. In some cases the public-key cryptography efficiently obtained similar or even greater than symmetric key encryption using keys smaller.

RSA Algorithm: A method to implement a public key cryptosystem whose security is based on the difficulty of factoring large prime numbers was proposed in [6]. *RSA* standsfor Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. It is possible to encrypt data and create digital signatures. *RSA* public key algorithm is the most widely used in the world. The encryption scheme uses RSA and signature of the fact that:

$$m^{ed} \equiv m(modn)$$

for m integer.

Encryption and decryption schemes are presented in Algorithms 1 and 2. Decryption works because

$$c^d \equiv (m^e)^d \equiv m(modn)$$

Encryption Algorithm
Input: RSA public key (n,e), Plain text m ∈ [0, n-1]
Output: Cipher text c
Begin
Compute c = m^e mod n
Return c
End

Algorithm.1: RSA Encryption

Decryption Algorithm
Input: Public key (n,e),Private key d, Cipher text c
Output: Plain text m
begin
Compute m = c^d mod n
Return m
End

Algorithm.2: RSA Decryption

ECC (Elliptic curve cryptography) Algorithm: In the mid-80 [7] and [8] proposed a method of cryptography based on elliptic curves ECC. This algorithm is mainly depending on the algebraic structure of elliptic curves. An *elliptic curve* is a plane curve which consists of the points satisfying the equation*:*

$$y^2=x^3+ax+b.$$

The efficiency of this algorithm is based on finding a discrete logarithm of a random element that is part of an elliptic curve. The applicability of the algorithms based on elliptic curves on devices with computational constraints argue that the efficiency of ECC cryptographic algorithm with key sizes of approximately 160 bits is the same obtained using the RSA algorithm with 1024 bit key. Key management algorithms are used to share secret keys, encryption algorithms enable a confidential communication and digital signature algorithms authenticate a participant communication as well as validate the integrity of the message. The procedures of decryption and encryption through elliptic curve are described in the algorithms 3 and 4.

Elliptic Curve Encryption

Input: Parameters field of elliptic curve (p, E, P, n), Public key Q, Plain text m
Output: Cipher text (C_1, C_2)
begin
Represent the message m as a point M in E (F_p)
Select $k \in R^{[1,n-1]}$.
Compute $C1 = kP$
Compute $C2 = M + kQ$.
Return ($C1$, $C2$)
end

Algorithm.3: ECC Encryption Algorithm

Elliptic Curve Decryption

Input: Parameters field of elliptic curve (p, E, P, n), Public key Q, Cipher text (C_1, C_2)
Output: Plain text m
begin
Compute $M = C2 - dC1$, and m from M.
Return (m).
end

Algorithm.4: ECC Decryption Algorithm

The pure text m is first represented as a point M and then encrypted by the addition to kQ.
Where k=randomly chosen Integer,
Q=Public Key.
The transmitter transmits the points $C1 = kP$ and $C_2 = M + kQ$ to receiver who uses his private key d to compute:

$$dC_1 = d(kP) = k(dP) = kQ$$

and then calculating $M = C_2 - kQ$. Hence an attacker who wants to read of M need to calculate kQ.
Compared to RSA, ECC has small key size, low memory usage etc. There are many advantages in the ECC which are represented in the figure.4.

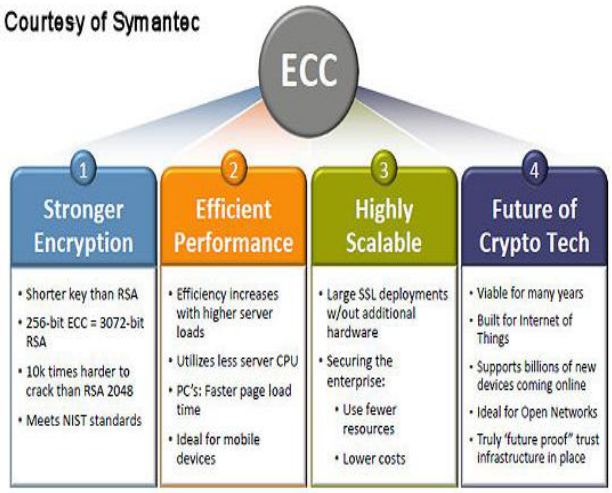

Fig.4. Advantages of using ECC Algorithm

On our research work we have noted that the energy consumption is less in ECC comparing to the RSA on the Handshake protocol.

Algorithm	Client	Server
RSA-1024	397.7 µJ	390.3 µJ
ECC-160	93.7 µJ	93.9 µJ

Table.1. Energy consumption on handshake protocol

IV. PROPOSED SCHEME

When the data is sending to the sensor to the base station the data must be confidential in the route between them. But if the data is passed through the malicious node it can read or modify the data. Proposed scheme keeps the data confidential from the source node to the base station at each step as follows:

a. A malicious node can enter our network and can send forge or confused data to the base station to be pretend as a authorized node.
b. It can also modify, insert or delete the data during transmission impersonated as a legal node.
c. Any unauthorized malicious node can send duplicate data and can attempt to repeat authorized data to the base station which is already send.
d. The sensor network must be robust menace if let a new node is added to the existing network.

ECC minimized the above said attacks at the Sensor Network and prevents the following by the below constraints:

- Confidentiality
- Authentication
- Data Integrity
- replay attack
- Non repudiation source

The key assumptions that want to be required in our scheme are:

- The unique id wants to be generated for each sensor.
- The sensor wants to be static and homogeneous.
- It should be ensured that adversary cannot
- compromise Sensor Nodes immediately after
- nodes are deployed.
- Each Sensor node has a comparator

Our scheme is based on Elliptic curve Cryptography algorithm for light weighted and resource constrained Sensor nodes with some modification. Each node is limited to broadcast the message only to the neighbor node only. In our scheme the algorithm takes place in the three step process:

Step.1:.Before the deployment of the sensor:

The Base Station select a large integer q, which is either prime number p or an integer of the form 2^m and elliptic curve parameter a and b for following equation. $Y^2 + xy = x^3 + ax^2 + b$. The base station generates public keys for each of the sensor nodes and for itself by following equation. P = n * G where n and p are private and public values respectively.

Step.2:.After the Deployment of the Sensor

Now every node of our static network broadcast their public value P to its neighboring nodes with its id. Now every node calculates its secret key by using following equation, let second node is the neighbor of the first node. Now every node has a secret key to exchange the message to each other with its id. Here every shows there confidentiality, integrity and authentications to each other.

Step.3:.Adding new node in to the existing network

Now if a new Sensor Node is deploys to the exiting one with the same values that is n_R, P_R and G. The neighbors generate the corresponding keys by using its previous value that is encrypted with its symmetric key.

V. RESULTS AND ANALYSIS

We used the Elliptic Curve Cryptography algorithm with little modification on Sensor Network. ECC algorithm depends for the effectiveness on the difficulty of the computing discrete logarithms, which increases the strength. The general query arise is how our scheme is better than conventional RSA in the sensor network. The reason is the public key cryptography algorithm is slower than symmetric key cryptography because it involves power function calculation that takes more execution time. ECC bits are two times better than RSA bits considering code size and power consumption. RSA involve power function calculation every time it encrypt and decrypt the data so it consume large amount of energy every time, Where as in the ECC does not involve power function calculation at sensor nodes as well as the by the above said steps it is clear that most of the calculation is done at the base station that has enough power for the calculation.

VI. CONCLUSION

The wireless sensor networks continue to grow and become widely used in many applications. The wireless sensor network suffers from many constraints such as storage capacity, processing capability, and, limited energy etc. In our scheme we have proposed a secured algorithm in the wireless sensor networks. In our framework we identify the steps which are required for the sensor. Hence we implement the power function on the base station. Our proposed scheme is not even securing the Network at some extent but it also helps to utilize the resources efficiently and also open the options that public key methods can be used for securing the Sensor Network. We have compared two schemes in this paper ECC, and RSA and found out that ECC is more advantageous compared to RSA. ECC bits is two times better than RSA bits when code size and power consumption are the factors of consideration. Our proposed scheme shows that after adding security by public key method energy consumption is slightly increased compared to symmetric key cryptography.

REFERENCE

[1]. Shish Ahmad, DR. Mohd. Rizwan beg,and Dr. Qamar Abbas,‖ Energy Saving Secure Framework for Sensor Network using Elliptic Curve Cryptography‖,IJCA Special Issue on "Mobile Ad-hoc Networks",21(2):167-172,2010.

[2] Kumuda T P, Mrs. Sridevi K.N,‖ Energy Efficient and Secure, Trusted network discovery for Wireless Sensor Networks ‖,IOSR Journal of Computer Engineering,12(4):101-111,2013.

[3]. Gaurav Sharma, Suman Bala, Anil K. Verma,‖ Security Frameworks for Wireless Sensor Networks-Review‖,International Conference on Communication, Computing & Security: 978 – 987,2012.

[4]. Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar,‖ SPINS: Security Protocols for Sensor Networks‖,Conference on Mobile Computing and Networking, 2001 Rome.

[5]. Gustavo S. Quirino, Admilson R. L. Ribeiro and Edward David Moreno,‖ Asymmetric Encryption in Wireless Sensor Networks‖,INTECH, Wireless Sensor Networks – Technology and Protocols.pp. 217-232.

[6]. R.L.Rivest,A.Shamir,and L.Adleman,‖A method for obtaining digital signatures and public-key cryptosystems‖,Communications of the ACM,21(2):120-126,1978.

[7] N. Koblitz. Elliptic curve cryptosystems. Mathematics of computation, 48(177):203–209, 1987.

[8] V. Miller. Use of elliptic curves in cryptography. In Advances in Cryptology – CRYPTO Proceedings, pages 417–426. Springer, 1986.

[9] Madhumita Panda, " Security in Wireless Sensor Networks using Cryptographic Techniques", Research paper, American Journal of Engineering Research , Volume-03, Issue-01, pp-50-56.